UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/697,397	10/29/2003	Laurence Lundblade	030457	7478

23696 7590 01/03/2007
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121

EXAMINER	
KOEMPEL THOMAS, BEATRICE L	
ART UNIT	**PAPER NUMBER**
2196	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	01/03/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 01/03/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

us-docketing@qualcomm.com
kascanla@qualcomm.com
t_ssadik@qualcomm.com

Office Action Summary	**Application No.** 10/697,397	**Applicant(s)** LUNDBLADE, LAURENCE	
	Examiner Bea Koempel-Thomas	**Art Unit** 2196	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *21 November 2005*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-45 are pending in this application and presented for examination.

Claim Objections

2. Claims 4, 7, 10, 13, 16, 20, 42 and 43 are objected to for the following informalities:

3. In claims 4, 10, 16, 20, and 43, "the modification detection technique" (line 1) lacks antecedent basis. In order to further prosecution, the examiner interpreted each instance as "a modification technique."

4. In claims 7 and 13, "the device" (line 2) lacks antecedent basis. In order to further prosecution, the examiner interpreted each instance as "a device."

5. In claim 42, "compromising" (line 1) appears to be a typographical error. In order to further prosecution, the examiner interpreted the word as "comprising." Examiner notes also that a "modification and authentication technique" is included in this claim, whereas similar claims have included a "modification detection and authentication technique."

6. Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-45 are rejected under 35 U.S.C. 103(a) as being obvious over Drews, U.S. Patent No. 6,477,645 B1, (hereinafter "Drews") in view of Bari et al., U.S. Patent Publication No. 2002/0023059 A1, (hereinafter "Bari").

9. Regarding **claim 1:** Drews discloses a method (col. 6 lines 15-16) for providing an application credential to an application running on a device (col. 2 lines 9-12), wherein the application credential is used by the application to authenticate to a data server (col. 3 lines 34-40 and col. 4 lines 30-36), the method comprising:

receiving a request to generate the application credential, wherein the request includes an application identifier (col. 3 line 15-19, transformation value generator, hash function, accepts (receives) input (request for application credential), a variable length amount of digital data (application identifier)); and

generating the application credential using the application identifier (col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (*see* Bari, ([0036] lines 2-5)).

10. Regarding **claim 7:** Drews discloses an apparatus (col. 2 lines 9-22) that operates to provide an application credential to an application running on a device (col. 2 lines 9-12), wherein the application credential is used by the application to authenticate to a data server (col. 3 lines 34-40 and col. 4 lines 30-36), the apparatus comprising:

receiving logic that operates to receive a request for the application credential, wherein the request includes an application identifier (col. 3 line 15-19, transformation value generator, hash function, accepts (receiving logic) input (request for application credential), a variable length amount of digital data (application identifier)); and

generating logic that operates to generate the application credential using the application identifier (col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating logic)).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to combine the teachings of Drews with the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (*see* Bari, ([0036] lines 2-5)).

11. Regarding **claim 13:** Drews discloses an apparatus (col. 2 lines 9-22) that operates to provide an application credential to an application running on a device (col. 2 lines 9-12),

wherein the application credential is used by the application to authenticate to a data server (col. 3 lines 34-40 and col. 4 lines 30-36), the apparatus comprising:

means for receiving a request for the application credential, wherein the request includes an application identifier (col. 3 line 15-19, transformation value generator, hash function, accepts (means for receiving) input (request for application credential), a variable length amount of digital data (application identifier)); and

means for generating the application credential using the application identifier and a master credential (col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (means for generating).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (*see* Bari, ([0036] lines 2-5)).

12. Regarding **claim 18:** Drews discloses a computer-readable media (col. 7 line 2) comprising instructions, which when executed by a processor in a device, provide an application credential to an application running on a device (col. 2 lines 9-12), wherein the application credential is used by the application to authenticate to a data server (col. 3 lines 34-40 and col. 4 lines 30-36), the computer readable media comprising:

instructions for receiving a request for the application credential, wherein the request includes an application identifier (col. 3 line 15-19, transformation value generator, hash function, accepts (receives) input (request for application credential), a variable length amount of digital data (application identifier)); and

instructions for generating the application credential using the application identifier and a master credential means for generating the application credential using the application identifier and a master credential (col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (*see* Bari, ([0036] lines 2-5)).

13. Regarding **claim 24:** Drews discloses a method for operating a credential server (col. 6 lines 15-16) to authenticate an application running on a device, wherein the application transmits a request for data to a data server and the request comprises an application credential, the method comprising:

receiving an application identifier in a request for a server credential (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 line 15-19, transformation value generator, hash function, accepts (receives) input (request for server credential), a variable length amount of digital data (application identifier));

generating the server credential using the application identifier (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating)); and

transmitting the server credential to the data server (col. 2 lines 9-32), wherein if the server credential and the application credential match, the application is authenticated (col. 4 lines 9-36, authorizing entity supplies (transmits) transformation value (server credential) to user/agent that submits (transmits) the transformation value (server credential) to the comparison system of user platform (data server), and comparison system compares the received transformation value (server credential) with the output of the transformation value generator (authentication credential)).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (*see* Bari, ([0036] lines 2-5)).

14. Regarding **claim 28:** Drews discloses an apparatus (col. 2 lines 9-22) for use with a credential server to authenticate an application running on a device, wherein the application transmits a request for data to a data server (col. 2 lines 34-42) and the request comprises an application credential (col. 3 line 24), the apparatus comprising:

first receiving logic that operates to receive an application identifier in a request for a server credential (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity, generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 line 15-19, transformation value generator, hash function, accepts (receiving logic) input (request for server credential), a variable length amount of digital data (application identifier));

generating logic that operates to generate the server credential based on the application identifier (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating logic)); and

transmitting logic that operates to transmit the server credential to the data server (col. 2 lines 9-32), wherein the data server matches the server credential to the application credential to authenticate the application (col. 4 lines 9-36, authorizing entity supplies (transmitting logic) transformation value (server credential) to user/agent that submits (transmitting logic) the transformation value (server credential) to the comparison system of user platform (data server), and comparison system compares the received transformation value (server credential) with the output of the transformation value generator (authentication credential)).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (*see* Bari, ([0036] lines 2-5)).

15. Regarding **claim 32:** Drews discloses an apparatus (col. 2 lines 9-22) for use with a credential server to authenticate an application running on a device, wherein the application transmits a request for data to a data server and the request comprises an application credential, the apparatus comprising:

means for receiving an application identifier in a request for a server credential (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 line 15-19, transformation value generator, hash function, accepts (means for receiving) input (request for server credential), a variable length amount of digital data (application identifier));

means for generating the server credential based on the application identifier (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (means for generating)); and

means for transmitting the server credential to the data server (col. 2 lines 9-32), wherein the data server matches the server credential to the application credential to authenticate the application (col. 4 lines 9-36, authorizing entity supplies (means for transmitting) transformation value (server credential) to user/agent that submits (means for transmitting) the transformation value (server credential) to the comparison system of user platform (data server), and comparison system compares the received transformation value (server credential) with the output of the transformation value generator (authentication credential)).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (*see* Bari, ([0036] lines 2-5)).

16. Regarding **claim 36:** Drews discloses a computer-readable media (col. 7 line 2) comprising instructions, which when executed by a processor in a credential server, operate to authenticate an application running on a device, wherein the application transmits a request for

data to a data server and the request comprises an application credential, the computer-readable media comprising:

instructions for receiving the application identifier in a request for a server credential (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 line 15-19, transformation value generator, hash function, accepts (receives) input (request for server credential), a variable length amount of digital data (application identifier));

instructions for generating the server credential based on the application identifier (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating)); and

instructions for transmitting the server credential to the data server (col. 2 lines 9-32), wherein the data server matches the server credential to the application credential to authenticate the application (col. 4 lines 9-36, authorizing entity supplies (transmits) transformation value (server credential) to user/agent that submits (transmits) the transformation value (server credential) to the comparison system of user platform (data server), and comparison system compares the received transformation value (server credential) with the output of the transformation value generator (authentication credential)).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (*see* Bari, ([0036] lines 2-5)).

17. Regarding **claim 40:** Drews discloses a method (col. 6 lines 15-16) for processing an application credential associated with an application running on a device, wherein the application credential is used by the application to authenticate to a data server, the method comprising:

receiving a request to generate the application credential, wherein the request includes an application identifier (col. 3 line 15-19, transformation value generator, hash function, accepts (receives) input (request for application credential), a variable length amount of digital data (application identifier)); and

generating the application credential using the application identifier (col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating).

transmitting a request for data to a data server (col. 2 lines 9-22), wherein the request comprises the application credential (col. 6 lines 15-44, authorizing entity identifies newly installed workstation requiring installation of a boot image (request for data), and transformation value (application credential) is necessary to obtain data).

(col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator

requesting a server credential from a credential server, wherein the request for the server credential comprises the application identifier (col. 3 line 16) and a token (col. 2 line 44) by which the data server authenticates itself (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 line 15-19, transformation value generator, hash function, accepts (receives) input (request for server credential), a variable length amount of digital data (application identifier));

generating the server credential using the application identifier (col. 3 lines 57-65, authorizing entity, an IT management organization or some other entity (credential server), generates and supplies (upon request) transformation values (server credentials) performing the same transformation as the transformation value generator, and col. 3 lines 15-33, transformation value generator, uses a variable length amount of digital data (application identifier) to create a transformation value (application credential) via hashing (generating)); and

transmitting the server credential to the data server (col. 2 lines 9-32),

matching the server credential with the application credential, wherein the application is authenticated if the two credentials match (col. 4 lines 9-36, authorizing entity supplies (transmits) transformation value (server credential) to user/agent that submits (transmits) the transformation value (server credential) to the comparison system of user platform (data server), and comparison system compares the received transformation value (server credential) with the output of the transformation value generator (authentication credential)); and

transmitting the data to the application (col. 6 lines 22-32).

Drews does not disclose a master credential.

Bari discloses a master credential ([0036] lines 10-23).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify Drews by the master credential taught by Bari for the benefit of identifying a particular user/device for authentication (*see* Bari, ([0036] lines 2-5)).

18. Regarding **claims 2, 8, 14, 22, and 41:** Drews discloses a one-way generation technique, so that the application identifier and the master credential can not be discovered from the application credential (col. 3 lines 15-33).

19. Regarding **claims 3, 9, 15, 19, and (42):** Drews discloses using a modification detection and authentication technique (col. 3 lines 49-65) to determine if the application or the application identifier has been modified (col. 3 lines 24-40) and prove the application is associated with the application identifier (col. 3 lines 24-40).

20. Regarding **claims 4, 10, 16, and 20:** Drews discloses the modification detection technique (col. 3 lines 49-65) is generated by a server that is distinct from a provider of the application (col. 3 lines 54-56).

21. Regarding **claims 5, 11, 17, 21, and 43:** Drews discloses the modification detection technique is a digital signature (col. 2 lines 42-52).

22. Regarding **claims 6, 12, 23, and 45:** Drews discloses the device is a wireless device (col. 2 lines 53-65).

23. Regarding **claims 25, 29, 33, 37, and 44:** Drews discloses receiving an authentication token (col. 2 line 44) that proves the request is associated with the application identifier (col. 2 lines 42-52).

24. Regarding **claims 26, 31, 35, and 39:** Drews discloses receiving the application credential (col. 3 lines 34-40); matching the application credential and the server credential (col. 3 lines 34-40); and transmitting an authorization to the data server to fulfill the data request if the application credential matches the server credential (col. 6 lines 15-54).

25. Regarding **claims 27, 30, 34, and 38:** Drews discloses generating the server credential (col. 3 lines 63-65) using a one-way generation technique, so that the application identifier and the master credential cannot be discovered from the server credential (col. 3 lines 15-33).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is:

- Thomlinson et al., U.S. Patent No. 6,272,631 B1, regarding protected storage of data.
- Donley et al., U.S. Patent Publication No. 2004/0180646 A1, regarding wireless authentication.
- Eggebraaten et al., U.S. Patent No. 7,146,635 B2, regarding authentication and authorization to access resources.
- Abgrall et al., U.S. Patent Publication No. 2003/0037237 A1, regarding computer device authentication.
- Khanna et al., U.S. Patent Publication No. 2005/0071677 A1, regarding a method to authenticate.

Please direct any inquiry concerning this communication or earlier communications from the examiner to Bea Koempel-Thomas whose telephone number is 571-270-1252. The examiner can normally be reached on Monday - Thursday & alternate Fridays; 0730 - 1700.

If attempts to reach the examiner by telephone are unsuccessful, please contact the examiner's supervisor, Nabil El-Hady, on 571-272-3963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

bkt
12/20/2006

NABIL M. EL-HADY
SUPERVISORY PATENT EXAMINER